

Vorname und Name: Murad Khasawneh
Anschrift: Goethestraße 73
D-63477 Maintal
Fachbereich: Soziologie
Matrikelnummer: 1583241

Hausarbeitsthema: 3002 - Spuren im Staub oder elektronische Fährten?
Seminarthema: Negative Utopien: Die Technologie der Überwachung
Veranstalter: Mans, Dieter
Veranstaltungszeitraum: Sommersemester 2003

Inhalt

1. Der Lauscher an der Wand.....	3
2. Überwachung der Telekommunikation.....	3
2.1. Funktionsweise des Telefons.....	4
2.2. Abhören des Telefons.....	4
2.3. Gegenmaßnahmen.....	5
2.4. Schlaglichter auf die Geschichte der Telekommunikation.....	5
2.5. Besonderheiten der Mobilfunktechnik.....	7
2.6. Ausschnitte aus aktuellen Gesetzestexten.....	9
2.6.1. Möglichkeiten.....	9
2.6.2. Anlässe.....	10
2.6.3. Grenzen.....	11
2.6.4. Bundesdatenschutzgesetz.....	12
2.7. Schauversuch zur Überwachung analoger Telefonanschlüsse.....	13
2.8. Knacken in der Leitung.....	14
3. Andere Mittel der (alltäglichen) Überwachung.....	16
3.1. Spione auf dem Schreibtisch.....	16
3.2. Spione in der Geldbörse.....	17
3.3. Videoüberwachung.....	18
3.4. Satellitengestützte Überwachung.....	20
3.5. Großer Lauschangriff.....	21
4. Kein Grund zu Paranoia.....	21
Danksagung.....	23
Urheberrechtlicher Hinweis.....	23

1. Der Lauscher an der Wand...

Diese Überschrift lädt ein, zu vervollständigen: „hört seine eigene Schand!“ Allerdings möchte ich weniger auf moralische Aspekte des Lauschens eingehen, sondern hauptsächlich auf die technischen Möglichkeiten der (Telefon-) Überwachung.

Weiter möchte ich den Blick auf einzelne eng damit verwobene rechtliche Voraussetzungen und Rahmenbedingungen werfen.

Besondere Beachtung soll hierbei die staatliche Überwachung der (Tele-) Kommunikation finden.¹

2. Überwachung der Telekommunikation

Briefpost kann man abfangen und öffnen.

Das Ministerium für Staatssicherheit tat dies in der DDR in nicht kleinem Umfang. Da sich wasserlöslich verklebte Briefe mittels Wasserdampf öffnen lassen, wurden Normbriefe sogar weitgehend automatisiert geöffnet und wieder verschlossen. Andere Klebstoffe lassen sich mittels Heißluft öffnen, auch dies zum Teil automatisiert. Insgesamt sollen etwa 90000 fremde Briefe täglich gelesen worden sein.²

Wenn sich der Inhalt nicht unbemerkt ermitteln läßt und man die Post längere Zeit beschlagnahmen muß, dürfte es den Kommunikationspartnern früher oder später auffallen.

Die Überwachung der Telekommunikation auf Basis von Telephonie³ bietet eine besonders interessante Möglichkeit: sie kann leicht unentdeckt vor sich gehen, da man die Leitung unterwegs anzapfen kann. Hierbei fällt die Manipulation der Leitung normalerweise nicht auf. Die Übertragungswege sind bekannt und bleiben längerfristig unverändert. Man muß nicht in den laufenden Betrieb eingreifen und verursacht keine Verzögerung in der Übermittlung.

¹ Aus naheliegenden Gründen beziehen sich die Betrachtungen hauptsächlich auf die Bundesrepublik Deutschland, sofern es sich nicht um allgemeine geschichtliche oder technische Aspekte handelt.

² Museumsstiftung Post und Telekommunikation (Herausgegeben von Joachim Kallinich und Sylvia de Pasquale): Ein offenes Geheimnis, Post und Telefonkontrolle in der DDR, 2. Auflage März 2003, Seite 63 (erhältlich im Museum für Kommunikation Frankfurt, vormals Deutsches Postmuseum, Schaumainkai 53 [Museumsufer], D-60596 Frankfurt am Main)

³ Man vergebe mir die wechselnde Schreibweise Telefon und Telephon. Ich wählte hier die Schreibweise Telephonie, um die Wortbedeutung der Fernübermittlung akustischer Phänomene hervorzustellen.

2.1. Funktionsweise des Telefons

Was ist ein Telefon? „Telephon“ setzt sich aus den dem Griechischen entlehnten Wortteilen tele = fern, weit und phone = Stimme zusammen.⁴ Also ein Fernsprechapparat.

Um dem Phänomen näher zu kommen, betrachten wir kurz die prinzipielle Funktionsweise des Apparates:

Ein Mikrofon nimmt die Schallwellen des Sprechers auf und verändert entsprechend die an der Telefonleitung anliegende Spannung.⁵ Am anderen Ende der Leitung versetzen diese Spannungsschwankungen einen Lautsprecher in Schwingungen und reproduzieren so die ursprünglichen Schallwellen.⁶

2.2. Abhören des Telefons

Da die den Schall übermittelnde Spannungsschwankung auf der vollen Länge der Leitung feststellbar ist, kann man sie auch an jeder Stelle der Leitung hörbar machen. So kann nicht nur ein Teilnehmer den jeweils anderen Gesprächspartner hören, sondern auch ein dritter unbemerkt mithören.

Im einfachsten Fall geschieht dies durch einen Mitbewohner im Nebenzimmer über einen parallel angeschlossenen Telefonapparat, wie man es zum Beispiel aus Kriminalfilmen kennt.⁷ Überneugierige Nachbarn, Spione oder staatliche Ermittlungsstellen schließen aber eher speziell zum Abhören konzipierte Apparate an die Telefonleitung im Keller, im Anschlußkasten an der Hauswand, im Verteiler auf der Straße oder in der Vermittlungsstelle an. Diese Apparate müssen nicht sehr aufwendig sein, aber so konzipiert, daß sie zum Einen nur das abzuhörende Gespräch hörbar machen oder aufzeichnen, ohne selbst ein Geräusch in die Leitung zu übertragen und zum Anderen der Leitung möglichst wenig Strom entnehmen, um sich nicht durch Beeinträchtigung der Leitungsqualität zu verraten. Man erreicht dies schon alleine durch Verwendung eines Übertragers oder Transformators, eventuell über einen hohen Widerstand an die Leitung gekoppelt, und eines nachgeschalteten Verstärkers oder Aufzeichnungsgerätes mit empfindlichem Eingang.

⁴ Dieses Vorkommen der Schreibweise *Telephon* erklärt sich selbst.

⁵ Das später erwähnte, von Bell entwickelte Gerät induzierte, angeregt durch Schallwellen mittels eines Magneten einen Strom in einer Spule und das identische Gegenstück am anderen Ende der Leitung erzeugte hieraus wieder Schallwellen – eine zusätzliche Stromversorgung war zunächst unnötig. Ein Nachbau dieses Gerätes kann im Museum für Kommunikation, Schaumainkai 53, Frankfurt am Main ausprobiert (sic!) werden.

⁶ Siehe auch Anhang „Vereinfachte Darstellung der Funktionsweise des Telefons“

⁷ Derart parallel angeschlossene Telefonapparate spielen hauptsächlich in amerikanischen Krimis und Serien eine Rolle. Hierzulande war es lange Zeit streng verboten, Telefonapparate parallel anzuschließen (was nicht heißt, daß es jetzt wirklich erlaubt wäre).

Moderne digitale Telekommunikationstechnik übermittelt Telefongespräche und andere Kommunikation digital, also in Form von Daten. Analog ist im wesentlichen nur noch die Leitung vom Teilnehmer bis zur Vermittlungsstelle. Wenn man einen digitalen Telefonanschluß, zum Beispiel einen ISDN-Anschluß abhören möchte, hört man mit herkömmlicher Technik nur ein Rauschen, das durch die digitale Datenübertragung entsteht. Um dies verwertbar zu machen, benötigt man eine spezielle Ausrüstung.

Moderne Ermittlungsbehörden quartieren ihre Mitarbeiter nicht im Keller ein, sondern lassen sich das Gespräch „frei Haus liefern“.⁸

2.3. Gegenmaßnahmen

Um ein Abhören des Gespräches zu erschweren, gibt es Möglichkeiten, es zu verschlüsseln. Einige Unternehmen haben sich darauf spezialisiert, ISDN-Telefone und Mobiltelefone zu entwickeln, die Gesprächsdaten verschlüsseln, um sichere Telefonkonferenzen führen zu können.

Beispielsweise bietet die Firma Rohde & Schwarz GmbH & Co. KG⁹ das in Zusammenarbeit mit dem Bundesministerium für Sicherheit in der Informationstechnik (BSI) für den Einsatz im ISDN konzipierte Kryptosystem ElcroDat 6-2¹⁰, unter weiteren Geräten auch ein hierzu kompatibles Mobiltelefon mit Verschlüsselung, an.

Natürlich gibt es auch andere Anbieter solcher Verschlüsselungstechnologien für die Telekommunikation, dieses Unternehmen nannte ich nur wegen seiner Zusammenarbeit mit dem BSI.

2.4. Schlaglichter auf die Geschichte der Telekommunikation

Man könnte den Beginn der Telekommunikation¹¹ auf eine Zeit zwischen 8000-6000 v.Chr.¹² datieren, aus der erste Tonmarken („Tokens“) im heutigen Nahen Osten gefunden wurden oder auf etwa 3700-2600 v.Chr., als solche Tokens in Umhüllungen aus Ton verschlossen wurden¹³. Diese Tokens stellen vermutlich Vorläufer der Schriftentwicklung in Mesopotamien, die wir oft mit den Sumerern assoziieren, dar.

⁸ Siehe „Ausschnitte aus aktuellen Gesetzestexten“

⁹ ROHDE & SCHWARZ GmbH & Co. KG, Mühlendorfstraße 15, D-81671 München, <http://www.rohde-schwarz.com>

¹⁰ <http://www.bsi.de/projekte/edat62>, 17.07.2003, 19:42 / [http://www.rohde-schwarz.fr/www/dev_center.nsf/html/nav.10.17&content=http://www.rohde-schwarz.fr/www/dev_center.nsf/html/news020703elcrodat6-2s-d?OpenDocument](http://www.rohde-schwarz.fr/www/dev_center.nsf/frameset?OpenAgent&website=com&navig=/www/dev_center.nsf/html/nav.10.17&content=http://www.rohde-schwarz.fr/www/dev_center.nsf/html/news020703elcrodat6-2s-d?OpenDocument), 17.07.2003, 20:20

¹¹ Achtung: Ich verwende Telekommunikation hier im Sinne von Mitteilungen über größere Distanz.

¹² Denise Schmandt-Besserat: How writing came about, Abridged edition of *Before Writing*, Volume 1: From Counting to Cuneiform, © 1992, 1996 by the University of Texas Press, First abridged edition, 1996, S. 8

¹³ Denise Schmandt-Besserat: How writing came about, S. 44

Genaugut könnte man den Zeitpunkt der ersten Telekommunikation früher datieren, wenn es gelänge, nachzuweisen, daß Menschen Nachrichten über größere Distanzen übermittelten, sei es durch Boten, die sich den Text frei oder mittels Gedächtnisstützen, wie Knoten in Schnüren oder Einkerbungen in Holz oder Knochen, merkten oder durch Rauchzeichen oder Trommeln...

Um den Bezug zu Überwachungstechnologien nicht ganz zu verlieren, breche ich meine Überlegungen hier ab und springe, die Entwicklung des Transportes und der Post¹⁴ außer Acht lassend, einige Jahrtausende vorwärts.

Der Erfindung des Telefons ging die gründliche Erforschung der Elektrizität und die Erfindung des Telegrafen voraus.

In diesem Zusammenhang zähle ich bekannte Personen und ihre Entdeckungen oder Erfindungen auf: Gilbert (Reibungsexperimente mit Bernstein, 1600), Guericke (Elektrifiziermaschine, 1672), van Musschenbroek / von Kleist (erster Kondensator, 1745), Franklin (Blitzableiter, 1752), Priestley (elektrische Leitfähigkeit von Holzkohle "The History of Electricity", 1766/1777), Coulomb (Torsionswaage, 1777), Galvani (elektrische Muskelkontraktion an Froschbeinen), Volta (elektrische Batterie, 1800), Soemmerling (1809, elektrolytischer Telegraph), Ørsted (experimenteller Nachweis des Magnetfeldes um einen stromdurchflossenen Leiter, 1819 oder 1820), Ampere (elektromagnetische Spule), Faraday (Induktionsgesetz, 1831), Morse (Telegraph, 1837), Wheatstone und Cooke (Telegraph, ebenfalls 1837)¹⁵

Trotzdem werden als Erfinder des Telefons meistens nur Alexander Graham Bell, der sein erstes Telefon 1872 baute¹⁶ und nachrangig Johann Philipp Reis erwähnt, der sein Telephon bereits am 26. Oktober 1861 im Physikalischen Verein zu Frankfurt am Main vorstellte¹⁷.

Wären das von Reis entwickelte, auf Kontaktunterbrechung basierende Gerät sich nicht durchsetzte, konnte Bell sein elektromagnetisches Telefon 1876 kurz vor Elisha Gray patentieren.¹⁸

Telefone waren billiger und einfacher zu bedienen, als Telegrafen. So erhielten sie schnell Einzug in Unternehmen und Privathaushalte. Die Verbindungen zwischen den Teilnehmern wurden in den Vermittlungsstellen von Hand hergestellt.

¹⁴ Nur des Name-Droppings wegen sei hier die Familie Thurn und Taxis erwähnt, die im Mittelalter und noch bis 1866 im Nachrichtenwesen Deutschlands und Mitteleuropas eine wichtige Rolle einnahm.

¹⁵ Diese Aufstellung geht zum Teil zurück auf: Katalog des Museum für Kommunikation: Museum und Microsoft Encarta Enzyklopädie 2002, "Telegraph" und M&PHY München: "Elektrizität", in Microsoft® Encarta® Professional 2002. © 1993-2001 Microsoft Corporation.

¹⁶ Jahreszahl aus Microsoft Encarta Enzyklopädie 2002, „Telefon“

¹⁷ In der mir vorliegenden Literatur wird der Begriff „Telephon“ im Zusammenhang mit dieser technischen Erfindung erstmalig von Reis erwähnt. Das Wort selbst war zuvor schon bekannt.

¹⁸ Katalog des Museum für Kommunikation: Museum, Braunschweig 1990, S.72ff

Am 12. März 1889 meldete Almon B. Strowger den Hebdrehwähler zum Patent an. Am 21.05.1900 nahm die Reichstelegraphenverwaltung eine Versuchsvermittlungsstelle in Betrieb, die auf diesem Gerät basierte. Ab 1905 wurde es im öffentlichen Fernsprechnetz eingesetzt und verdrängte die manuelle Telefonvermittlung, bekannt als das Fräulein vom Amt.¹⁹

Die grundlegende Funktionsweise des Telefons änderte sich bis heute kaum, allerdings wurde das deutsche Fernsprechnetz nach der Wiedervereinigung flächendeckend digitalisiert. Zwar arbeitete das Netz schon länger teilweise digital, doch jetzt ist nur noch der letzte Abschnitt zum Teilnehmer analog und dies auch nur, falls dieser nicht mindestens über ISDN verfügt.

Digitale Übermittlung des Gesprächs bedeutet konkret, daß kontinuierlich Frequenz und Amplitude der elektromagnetischen Schwingung auf der Telefonleitung, also Tonhöhe und Lautstärke des aufgenommenen Tons nach einem genormten Verfahren in Meßwerte codiert werden, die dann ohne Qualitätsverluste zur Gegenstelle übertragen und dort wieder in elektromagnetische Schwingungen umgesetzt und hörbar gemacht werden.

2.5. Besonderheiten der Mobilfunktechnik

Mobiltelefone entscheiden sich vor Allem in einer besonderen Eigenschaft von ortsgebundenen Apparaten: man kann sie beliebig mitnehmen. An herkömmlichen Telefonanschlüssen kann man auch Schnurlostelefone betreiben. Da sie jedoch nur eine geringe Reichweite (In der Regel bis zu wenigen hundert Metern, höchstens bis zu wenigen Kilometern²⁰) aufweisen und an einen herkömmlichen Telefonanschluß gebunden sind, betrachte ich sie ebenfalls als ortsgebundene Telefone.

Die im modernen deutschen Sprachgebrauch als „Handy“ bekannten Mobiltelefone funktionieren in der Regel im gesamten Bundesgebiet, darüber hinaus je nach Mobilfunkvertrag und Abkommen des Netzbetreibers in den meisten Staaten der Welt, abhängig von der jeweiligen Infrastruktur, mindestens in den Ballungszentren und touristisch erschlossenen Siedlungsgebieten.

Theoretisch kann ein Teilnehmer mit seinem Mobiltelefon von einem beliebigen Ort aus telefonieren. In der Praxis muß er sich hierzu jedoch im Erfassungsbereich einer Sende- und Empfangseinrichtung seines Netzbetreibers oder dessen Vertragspartners aufhalten. Darüber hinaus muß die entsprechende Sende- und Empfangsanlage des Mobilfunknetzes sein Mobiltelefon, genau

¹⁹ Helmut Gold, Anette Koch (Herausgeber): Fräulein vom Amt, München 1993, S. 88 / Katalog des Museum für Kommunikation: Museum, S.78

²⁰ In der BRD zugelassene Schnurlostelefone haben in der Regel eine Reichweite von bis zu 300m.

genommen die auf der als SIM-Karte²¹ bekannten Chip-Karte gespeicherten Identifikationsmerkmale, registriert und ihn als berechtigten Teilnehmer erkannt haben. Er muß ins Netz eingebucht sein.

Dies hat hauptsächlich zwei Gründe: erstens will kein Telekommunikationsunternehmen seine Leistungen bereitstellen, ohne mit dem Teilnehmer abrechnen zu können, zweitens muß das Mobilfunknetz den Teilnehmer finden, um ihn mit einem Gesprächspartner verbinden zu können. Letzteres ist vor Allem wichtig, wenn der Mobilfunkteilnehmer angerufen wird. Sobald sich das Mobiltelefon im Netz einbucht, wird der Teilnehmer identifiziert und seine Position²² bestimmt. Jetzt findet ihn das Mobilfunknetz, wenn jemand versucht, ihn anzurufen, oder ihm eine Kurznachricht („SMS“) zu senden. Der Anrufer muß also den Aufenthaltsort des Mobilfunkteilnehmers beziehungsweise die Vorwahl seines augenblicklichen Standortes nicht kennen, was der leichteren Erreichbarkeit dient.

Der Umstand, daß das Mobilfunknetz den Aufenthaltsort eines Mobiltelefons kennt, eröffnet weitere Möglichkeiten:

Das Mobilfunkunternehmen O2 bietet auf seiner Homepage²³ die praktische Funktion „Handy-Finder“ an: Wenn man sein Handy verlegt hat, kann man, vorhergegangene Registrierung für diesen Dienst vorausgesetzt, sein Gerät orten lassen.²⁴ Das funktioniert allerdings nur, wenn das Gerät noch eingeschaltet und im Netz von O2 eingebucht ist. Auf einem Stadtplan bekommt man dann die ungefähre Position auf einige hundert Meter genau angezeigt. So weiß man wenigstens, ob man es eher am Arbeitsplatz, bei Freunden oder im Garten liegen ließ.²⁵

Da das Netz jederzeit den Standort kennt, kann auch bei staatlichen Ermittlungen darauf zurückgegriffen werden.

Eine andere Möglichkeit, Mobiltelefone zu überwachen, besteht im Einsatz eines als IMSI-Catcher bekannten Gerätes, das sich zwischen Mobiltelefon und Mobilfunknetz schaltet. Dies wird erreicht, indem dieses Gerät dem Mobiltelefon eine näher liegende Sendeeinrichtung des Netzes und dieser gegenüber das Mobiltelefon simuliert.²⁶

Einerseits erhält man so die Kennungen aller im Wirkungsbereich (das sollen etwa 100m sein) befindlichen Mobiltelefone, zum Anderen laufen so deren Gespräche alle über dieses Gerät. Es soll möglich sein, die Mobiltelefone aufzufordern, die Verschlüsselung zu deaktivieren, ohne daß der Teilnehmer

²¹ SIM = Subscriber Identity Module

²² Es wird die Funkzelle bestimmt, in der der Teilnehmer sich aufhält.

²³ <http://www.o2online.de/o2/kunden/myo2/postpaid/handy/handyfinder/index.html> , 29.04. / 12.05.2003

²⁴ Zum erfolgreichen Registrieren muß man eine SMS empfangen.

²⁵ Siehe Anhang „O2 Handy-Finder“

²⁶ IMSI = International Mobile Subscriber Identity (Internationale Kennungen für mobile Teilnehmer)

hiervon Kenntnis erlangt. Der Einsatz solcher Geräte zur Ermittlung des Standortes eines Mobiltelefons ist Ermittlungsbehörden aufgrund §100i StPO²⁷ unter bestimmten Voraussetzungen erlaubt. Da es sich um ein transportables Gerät handelt, das sich problemlos in ein Fahrzeug einbauen ließe, kann man sich damit in die Funkzelle begeben, in der der gesuchte Teilnehmer sich befindet, um ihn noch präziser zu orten.

Ein Problem scheint allerdings zu sein, daß das Gerät sämtliche Mobiltelefone im Wirkungsbereich umlenkt und so auch die Kennungen unbeteiligter aufzeichnet sowie deren Standorte verraten kann. Deshalb sind die Daten Unbeteiligter sofort wieder zu löschen. Darüber hinaus soll das Gerät für kurzzeitige Probleme beim Verbindungsaufbau sorgen, ohne jedoch laufende Gespräche zu unterbrechen.²⁸

2.6. Ausschnitte aus aktuellen Gesetzestexten

Im modernen Rechtsstaat, überläßt man den Eingriff in Persönlichkeitsrechte nicht dem Zufall. Deshalb regeln Gesetze Anlässe und Grenzen der Telefonüberwachung.

2.6.1. Möglichkeiten

Die Möglichkeiten moderner digitaler Telekommunikationsnetze schlagen sich auch in Gesetzestexten nieder.

Die TKÜV (Telekommunikations-Überwachungs-Verordnung) spricht hier beispielsweise wörtlich von einer „Kopie der Telekommunikation“:

„Zur Umsetzung einer Überwachungsmaßnahme hat der Verpflichtete der berechtigten Stelle am Übergabepunkt eine vollständige Kopie der Telekommunikation bereitzustellen, die über seine Telekommunikationsanlage unter der in der Anordnung angegebenen Kennung abgewickelt wird.“²⁹

Moderne Vermittlungsstellen arbeiten vollständig digital. Ihre Funktionsweise hängt maßgeblich von ihrer Programmierung ab.

Um neue Funktionen, wie netzseitige digitale Anrufbeantworter³⁰ oder Änderung der Rufweiterleitung über das Internet, zu realisieren, kann die Software der Vermittlungstechnik angepaßt werden. Um eine Kopie der Telekommunikation bereitzustellen, muß im Prinzip nur der entsprechende

²⁷ siehe „Ausschnitte aus aktuellen Gesetzestexten“

²⁸ Meine „Kenntnisse“ zum IMSI-Catcher beziehen sich hauptsächlich auf die in Presse und Fernsehen diskutierten Eigenschaften und Probleme seines Einsatzes.

²⁹ §5 TKÜV vom 22.01.2002, Absatz 1, Satz 1 (Erhältlich z.B. über <http://www.bmwi.de/Homepage/Politikfelder/Telekommunikation%20&%20Post/Telekommunikationspolitik/R echtsgrundlagen.jsp>)

³⁰ z.B. T-Net-Box der Telekom

Datenstrom vervielfältigt und an eine geeignete Schnittstelle weitergeleitet werden, von der aus er dann weiter verarbeitet werden kann.³¹

Die Regulierungsbehörde für Telekommunikation und Post ist maßgeblich an der Entwicklung der zu Grunde liegenden Technische Richtlinie und deren Anpassung an den jeweiligen Stand der Technik beteiligt:

„Die Regulierungsbehörde für Telekommunikation und Post erarbeitet unter Beteiligung der Verpflichteten, der Hersteller der technischen Einrichtungen, der berechtigten Stellen sowie der Hersteller der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen einen Vorschlag für eine Technische Richtlinie, in der die technischen Einzelheiten zu [...] sowie die erforderlichen technischen Eigenschaften der Anschlüsse nach [...] in Abhängigkeit von den den Telekommunikationsanlagen zugrunde liegenden Technologien festzulegen sind. Dabei sind die vorhandenen Standards soweit wie möglich zu berücksichtigen. In gleicher Weise ist die Technische Richtlinie an den jeweiligen Stand der Technik anzupassen.“³²

Auf diese Weise werden Technik und Verfahren zur Überwachung der Telekommunikation immer dem Stand der Technik angepaßt, ohne diese selbst direkt im Gesetzestext zu beschreiben. Dieses Vorgehen ist schneller und flexibler, als wenn wenig sachkundige Parlamentarier technische Verfahren festlegen müßten.

Paragraph 100i der Strafprozeßordnung zur Ortung von Mobiltelefonen:

„(1) Durch technische Mittel dürfen

- 1. zur Vorbereitung einer Maßnahme nach §100a die Geräte- und Kartennummer sowie*
- 2. zur vorläufigen Festnahme nach §127 Abs. 2 oder Ergreifung des Täters auf Grund eines haftbefehls oder Unterbringungsbefehls der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden.“³³*

Diese Regelung ist recht neu und legalisiert die Nutzung des IMSI-Catchers.

2.6.2. Anlässe

Natürlich könnte man annehmen, jedes Telefongespräch würde jederzeit aufgezeichnet und archiviert, für den Fall, daß man es als Beweismittel für einen Strafprozeß benötigt.

Ja, vielleicht wird jedes Gespräch abgehört. Rein technisch wäre eine vollständige Aufzeichnung sämtlicher Telefonate des gesamten Telefonnetzes leicht zu realisieren, wenn auch mit einem gewissen Aufwand verbunden. Für legale Überwachung der Telekommunikation gibt es jedoch genaue gesetzliche Regelungen³⁴. Im Falle der Ermittlungen oder Beweissicherung für einen Strafprozeß gibt es beispielsweise folgende Regelung:

³¹ Die technische Vorgehensweise zur Erstellung dieser Kopie der Telekommunikation konnte ich bisher nicht recherchieren.

³² §11 TKÜV vom 22.01.2002

³³ §100i StPO (Strafprozeßordnung) Stand 15. Februar 2003, Absatz 1

„Die Überwachung und Aufzeichnung der Telekommunikation darf angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand als Täter oder Teilnehmer 1. a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates [...] begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.[...]“³⁵

Dies klingt recht ungenau, beinahe beliebig. Allerdings müßte die Polizei oder Staatsanwaltschaft schon glaubhaft machen, daß ein begründeter Verdacht besteht, daß der abzuhörende Teilnehmer zum Beispiel den Staat und seine Symbole verunglimpft³⁶.

2.6.3. Grenzen

Die Überwachung hat gesetzliche Grenzen.

Man könnte meinen, diese Aussage sei banal. Der Stellenwert dieser gesetzlichen Grenzen wird aber daran deutlich, daß diese im Grundgesetz festgestellt werden.

In Artikel 10 heißt es zum Brief-, Post- und Fernmeldegeheimnis:

„(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.“³⁷

Erst nachdem die grundsätzliche Unverletzlichkeit der Privatsphäre festgestellt wurde, werden dem Staat Möglichkeiten eröffnet, in diese doch einzugreifen: „(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden.“³⁸

Auf diese Weise scheint das Brief-, Post- und Fernmeldegeheimnis gleich wieder aufgeweicht zu werden, kann der Gesetzgeber hierzu doch beliebig Gesetze erlassen. Genau darin liegt die Absicht dieser Passage – der Staat kann eben nicht einfach beliebig in Grundrechte einzelner eingreifen ohne Spuren zu hinterlassen, sondern muß dies für alle Bürger gleichermaßen und für Jedermann nachlesbar durch Gesetze regeln.

In der Strafprozeßordnung findet sich beispielsweise folgende Regelung:

„Die Überwachung und Aufzeichnung der Telekommunikation (§100a) darf nur durch den Richter angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch von der Staatsanwaltschaft getroffen werden. Die Anordnung der Staatsanwaltschaft tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird.“³⁹

³⁴ Das Grundgesetz sieht vor, daß der Staat in die Rechte seiner Bürger nur aufgrund von Gesetzen eingreifen darf, siehe auch den Abschnitt „Grenzen“.

³⁵ Auszugsweise §100a StPO (Strafprozeßordnung) Stand 15. Februar 2003, Absatz 1

³⁶ Verunglimpfung des Staates und seiner Symbole, §90a StGB (Strafgesetzbuch), Stand 01. September 2002

³⁷ Art 10 Grundgesetz, Stand 15.10.2002, Absatz 1

³⁸ Art 10 Grundgesetz, Stand 15.10.2002, Absatz 2, Satz 1

³⁹ §100b StPO (Strafprozeßordnung) Stand 15. Februar 2003, Absatz 1

Artikel 97 des Grundgesetzes formuliert die Unabhängigkeit der Richter:
„(1) Die Richter sind unabhängig und nur dem Gesetze unterworfen.“⁴⁰

In diesem Rahmen wird deutlich, daß rechtmäßige Überwachungsmaßnahmen an Bedingungen geknüpft sind und sich aufgrund der damit verbundenen Verfahren gewissermaßen selbst dokumentieren.

Wann, wie und ob Betroffene hiervon Kenntnis erhalten steht auf einem anderen Blatt. Zwar ist grundsätzlich eine Information des Betroffenen nach Abschluß der Maßnahmen gesetzlich vorgeschrieben, jedoch in Ausnahmefällen Möglichkeiten zur Verzögerung derselben vorgesehen...

§101 StPO regelt die Benachrichtigung Betroffener wie folgt:

„(1) Von den getroffenen Maßnahmen [...] sind die Beteiligten zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit, von Leib oder Leben einer Person [...] geschehen kann.“⁴¹

Aktuelle Entwicklungen lassen vermuten, daß in diesem Sinne es gemäß Radio Eriwan heißt: „Im Prinzip ja. Aber...“⁴²

Da man die Benachrichtigung quasi bis zum jüngsten Tage hinauszögern kann⁴³, besteht zumindest potenziell die Möglichkeit, daß Betroffene nie etwas davon erfahren.

2.6.4. Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz soll den Einzelnen vor einer Beeinträchtigung seiner Persönlichkeitsrechte durch den Umgang mit seinen personenbezogenen Daten schützen.

Im Zentrum dieses Gesetzes stehen die Einwilligung des Betroffenen, Vermeidung oder sparsame Speicherung von personenbezogenen Daten sowie ein Recht auf Auskunft an den Betroffenen sowie eine Überwachung durch Datenschutzbeauftragte in Unternehmen, Behörden und Datenschutzbeauftragte des Landes und des Bundes.⁴⁴

Die Notwendigkeit des Bundesdatenschutzgesetzes ergibt sich aus den Möglichkeiten der elektronischen Datenverarbeitung.

Solange Karteien und Kataloge grundsätzlich von Hand durchsucht werden mußten, wenn man darin enthaltene Daten zusammentragen und abgleichen wollte, lohnte sich der Aufwand nur in begründeten Einzelfällen.

⁴⁰ Art 97 Grundgesetz, Stand 15.10.2002, Absatz 1

⁴¹ §101 StPO (Strafprozeßordnung) Stand 15. Februar 2003, Absatz 1

⁴² Da war doch etwas in den Medien zur Problematik „Großer Lauschangriff“... hierzu mehr unter „Großer Lauschangriff“.

⁴³ wobei alles weiterhin dokumentiert wird, nur eben unter Verschluss bleibt

⁴⁴ Der Bundesbeauftragte für den Datenschutz, BfD-Info 1, Bundesdatenschutzgesetz – Text und Erläuterung -, Dresden 2003, S. 56 ff; insbesondere §§1, 4, 4a, 4f

Computer können elektronische Datenbanken schnell und ohne großen personellen Aufwand nach beliebigen Kriterien sortieren und Daten miteinander verknüpfen. Behörden, aber auch private Datensammler können so aus vorhandenen Daten neue Schlüsse ziehen und so Erkenntnisse über die betroffenen Personen erhalten, die über die ursprünglich in den einzelnen Datensätzen gespeicherten Informationen hinausgehen.

Die Einwilligung des Betroffenen, Vermeidung oder sparsame Speicherung von personenbezogenen Daten ist deshalb besonders wichtig, weil die Verknüpfung erst einmal gespeicherter Daten so eine unüberschaubare Vielfalt neuer Daten erzeugen kann. Dies ist besonders dann der Fall, wenn ursprünglich nicht miteinander verbundene, Datenbanken zusammengeführt werden. Diese müssen auf den ersten Blick kaum Gemeinsamkeiten aufweisen, wie zum Beispiel Daten des Melderegisters und Mietspiegel, die aufgrund ihrer Verknüpfung eine Abschätzung der gezahlten Mieten einzelner Personen zulassen und so deren wirtschaftliche Gesamtsituation erraten lassen.

Weiter will ich auf Aspekte des Datenschutzes nicht eingehen, um zum zentralen Thema, der Überwachung der Telekommunikation zurückzukehren.

2.7. Schauversuch⁴⁵ zur Überwachung analoger Telefonanschlüsse

Im folgenden schildere ich meine Demonstration zum Abhören von analogen Telefonanschlüssen anhand eines Brettes mit zwei aufgemalten Wohn- oder Bürohäusern und einer aufgemalten Vermittlungsstelle.⁴⁶

Benötigte Geräte und Hilfsmittel:

Telefonanlage mit Anschlüssen für analoge Teilnehmer
Fernmeldeinstallationsleitung
Löt- oder Schraub-Verteiler
TAE-Dosen
Prüfkopfhörer
Übertrager, Vorverstärker, Verstärker und Lautsprecher für das Auditorium

Vorbereitung:

Man montiere ein Brett aufrecht an ein Gestell, schraube einige Telefondosen darauf, füge Telefonverteiler hinzu und befestige die Telefonanlage auf der Rückseite. Nun werden die Telefondosen über die Verteiler mittels Fernmeldeinstallationsleitung mit der Telefonanlage verbunden. Zum Schluß

⁴⁵ Im Handzettel vom 12.05.2003 nannte ich dies noch fälschlich „Laborversuch“. Die geänderte Überschrift trägt dem Umstand Rechnung, daß es sich aber nicht tatsächlich um einen Versuch, sondern eine Demonstration handelt.

⁴⁶ Foto schlechter Qualität: Siehe Anhang „Foto zum Laborversuch“

zeichnet man die Gebäude auf das Brett, zum Beispiel zwei Wohn- oder Bürogebäude und ein Gebäude, das die Vermittlungsstelle symbolisiert.

Durchführung:

Auf eine Verbindung zum öffentlichen Fernsprechnetz kann und sollte⁴⁷ verzichtet werden. An die Telefondosen werden Telefone angeschlossen. Die Funktion des Aufbaus kann durch interne Telefonate demonstriert werden.

Jetzt kann ein simuliertes Gespräch zwischen zwei Teilnehmern mittels Prüfkopfhörer abgehört werden.

Eine einfache Abhöreinrichtung, im Wesentlichen bestehend aus einem Widertsand und einem Übertrager, Verstärker und Lautsprecher ermöglichen es dem Publikum, an diesem „Lauschangriff“ teilzuhaben.⁴⁸

Kurze Zusammenfassung der Vorführung, die am 13.05.2003 in Raum 102a im Turm stattfand:

Auf einem Tisch stellte ich die auf ein Brett montierte Telefonlandschaft auf. Die tatsächlich aus einem Übertrager mit vorgeschaltetem Widerstand und einem modifizierten Telefonverstärker bestehende Abhöreinrichtung war über Pegelwandler, Mischpult und ein Gerät zur Unterbrechung von Rückkopplungen an die im Raum fest installierte Verstärkeranlage angeschlossen. Zum Abgreifen des Signals an den Verteilern waren zwei Leitungen mit Krokodilklemmen angebracht.

Insgesamt waren vier Telefone angeschlossen. Eines behielt ich direkt am Tisch, ein Gerät mit verlängerter Leitung ließ ich nach hinten weiterreichen und zwei Stück verteilte ich in der ersten Sitzreihe.

Kurz demonstrierte ich, daß man tatsächlich miteinander telefonieren konnte. Per Videokamera konnte ich Ausschnitte der Verteiler, in denen ich das Telefongespräch „anzapfte“ über die im Raum installierten Fernseher zeigen.⁴⁹ Ich zeigte, daß es möglich war, Telefonate im Haus oder in der Vermittlung abzuhören. Außerdem zeigte ich die Möglichkeit auf, eine Leitung so in ein anderes Gebäude zu rangieren (in den Verteilern „durchzuverbinden“), daß es möglich ist, einen Anschluß von einem beliebigen Ort aus abzuhören.

2.8. Knacken in der Leitung

Im Anschluß an die Veranstaltung sprachen mich einige Seminarteilnehmer an, ob bestimmte Störungen in der Telefonleitung auf eine Abhörmaßnahme schließen lassen.

⁴⁷ Sonst könnte es vielleicht passieren, daß versehentlich oder absichtlich eine Telefonverbindung mit einem uneingeweihten Teilnehmer zustande kommt, deren Inhalt dem Auditorium unangebrachter Weise zu Ohren kommt.

⁴⁸ Grafik hierzu: Siehe Anhang „Schematische Darstellung einer einfachen Abhöreinrichtung“

⁴⁹ Das Videobild war wohl, laut einzelner Rückmeldungen, auch aufgrund geringer Farbsättigung, nur bedingt aufschlußreich...

Wahrscheinlich nicht! Beim Abhören von Telefongesprächen soll natürlich niemand etwas mitbekommen, deswegen werden Abhörmaßnahmen so gestaltet, daß sie die Leitungsqualität nicht beeinträchtigen. Wenn das Telefonnetz allerdings derart marode ist, daß jede Arbeit daran Störungen verursacht, wird es vielleicht bei Abhörmaßnahmen ebenfalls zu Knacken in der Leitung kommen. Aber gestörte Leitungen sind genauso wenig Indiz für Abhörmaßnahmen, wie gute Verbindungen darauf hinweisen, daß keine Abhörmaßnahmen stattfinden.

Einige Beispiele für Leitungsstörungen und deren Ursachen:

Rhythmisches Klopfen während oder nach der Wahl bis zur Verbindung wird heute in der Regel nur bei Auslandsverbindungen auftreten, die teilweise noch über „alte“ analoge Telefonnetze oder Netzabschnitte laufen (eventuell auch große analoge Telefonanlagen, die in einigen Unternehmen und Behörden noch bis zur endgültigen Abschreibung oder bis zum Totalausfall weiter betrieben werden).

Fremde Telefongespräche im Hintergrund, aber eventuell recht deutlich verständlich, kommen in der Regel dadurch zustande, daß Leitungen über eine gewisse Distanz parallel verlaufen und das Magnetfeld des elektrischen Stromes einer Leitung in einer benachbarten Leitung wieder einen entsprechenden elektrischen Strom erzeugt.⁵⁰ Tritt dies nur hin und wieder auf, hilft es meistens, das Gespräch zu beenden und den Gesprächspartner erneut anzurufen, da dann wahrscheinlich unterwegs eine andere Leitung verwendet wird. Hört man an einem Anschluß ständig fremde Gespräche, eventuell gerade die seiner Nachbarn, deutet dies auf einen Mangel in der Gebäudeverkabelung hin. Am Besten spricht man dann seine Telefongesellschaft an.⁵¹

Knackende Leitungen sind meistens eine Folge alter oder schadhafter Leitungen, oxidierter, locker gewordener Verbindungen oder anderer technischer Fehler. Hin und wieder überschätzen sich fleißige Heimwerker und verlegen Leitungen in ihrem Haus selbst. Selten manipulieren „nette“ Nachbarn die Leitung, um auf fremde Kosten zu telefonieren – auch hierfür sind erst einmal die Telekommunikationsunternehmen zuständig.

⁵⁰ Stromschwankungen verursachen Schwankungen im Magnetfeld, die einen wechselnden Strom in der anderen Leitung induzieren...

⁵¹ Die Telekom ist in den meisten Fällen Eigentümer des Telefonnetzes und somit meistens zuständig. Selten ist der Gebäudeeigentümer oder ein anderes Unternehmen Eigentümer der Leitungen. Man sollte zuerst sein Telekommunikationsunternehmen, im Zweifel die Telekom fragen – Fragen alleine kostet nichts und kann durchaus bilden.

3. Andere Mittel der (alltäglichen) Überwachung

Es gibt Angelegenheiten, die bespricht man nicht am Telefon. Daß Telefonate potentiell abgehört werden können, gehört mittlerweile zum Allgemeinwissen. Viele Möglichkeiten zur Überwachung – nicht nur durch staatliche Organe – ignorieren wir im Gegenzug oder nehmen sie bereitwillig in Kauf.

3.1. Spione auf dem Schreibtisch

Spricht man von staatlichen Überwachungsmaßnahmen, denkt man vor Allem an die bereits beschriebene Telefonüberwachung in Form bloß passiven Abhörens geführter Telefonate oder das Ausspähen von eMails zum Beispiel durch Projekte, wie „Carnivore“. Zum Belauschen in geschlossenen Räumen geführter Gespräche müßte jedoch erst einmal jemand in die Wohnung bzw. das Büro eindringen. Die Möglichkeit bestünde, es wäre jedoch ein größerer Aufwand vonnöten, da hierbei schließlich keine Spuren hinterlassen werden sollen, die auf solche Maßnahmen hindeuten.

Diese Überzeugung⁵² ist jedoch nur zum Teil richtig!

Moderne Telefonanlagen verfügen über umfassende Fernwartungsfunktionen, die oft auch Funktionen beinhalten, die das Abhören eines Raumes über angeschlossene Telefone von Außen unterstützen.⁵³ Kleine Telefonanlagen, wie sie oft auch in Privathaushalten vorkommen, setzen hierzu in der Regel die Mitwirkung⁵⁴ eines an die Telefonanlage angeschlossenen Teilnehmers voraus. Größere Telefonanlagen lassen sich meistens ohne Zutun des Kunden aus der Ferne warten. Große Telefonanlagen mit mehreren tausend Teilnehmern können untereinander vernetzt werden und bilden so oft ganze Unternehmens-Telefonnetze, die bisweilen aus Anlagen verschiedener Hersteller bestehen und weltweit über unzählige Filialen verteilt sein können. Solche Anlagen verfügen teilweise über genormte serielle Schnittstellen, die den Anschluß eines Computers zur Programmierung erlauben. Statt dessen kann dort ebenso gut ein Modem angeschlossen werden, das über eine Nebenstellen-Rufnummer der Telefonanlage angerufen werden kann. Ein Mitwirken ist den Unternehmen nicht zuzumuten. Die Entscheidungsträger verfügen meistens nicht über Kenntnisse, die ihnen eine Kontrolle der Servicearbeiten ermöglichen würden und wünschen, daß ein Anruf der Hotline genügt, um die Arbeiten ihren Erfordernissen entsprechend ausführen zu lassen. Natürlich benötigt man zur Manipulation der Anlage Paßworte, vielleicht sogar spezielle Wartungsprogramme und natürlich Kenntnisse über den Anlagentyp

⁵² Die meisten Menschen, mit denen ich über das Thema sprach, vertraten zuvor eingeführte Ansicht.

⁵³ Bei herkömmlichen Telefonen ist es hierzu zusätzlich erforderlich, den Hörer abzunehmen oder die Freisprechfunktion zu aktivieren.

⁵⁴ - zur Not durch Täuschung des Mitwirkenden -

und den kundenspezifischen Ausbau der Anlage.⁵⁵ Ohne auf Methoden hierzu einzugehen merke ich an, daß man sich natürlich die Mitwirkung eingeweihter Personen sichern kann.

Da größere Telefonanlagen oft über Durchsage, Freisprech- und Mithörfunktionen verfügen, die sich je nach Programmierung auch unbemerkt aktivieren lassen⁵⁶, könnte man so auch ohne (Richt-) Mikrofone, „Wanzen“, Körperschallmikrofone, lasergestützte Abhörgeräte oder ähnliche Geräte einzusetzen, Gespräche abhören.

Handelsübliche Anrufbeantworter verfügen in der Regel ebenfalls über Raumabhörfunktionen. Diese lassen meistens mehrere Falscheingaben des Codes, der oft nur drei oder vier Ziffern lang ist, pro Anruf zu, bevor die Verbindung getrennt wird. Über ähnliche Funktionen verfügt auch so manches ISDN-Telefon.⁵⁷ Sofern das Gerät stumm gestellt ist oder die Mithörfunktion erst nach dem Pfeifton aktiviert, kann man die Raumabhörfunktion leicht ausnutzen.

Sobald ein mit dem Internet verbundener PC mit einer Webcam, oder einer anderen digitalen Camera verbunden ist, besteht sogar die Möglichkeit, mittels geeigneter Software (eines Virus oder eines sogenannten Trojaners) deren Bilder über das Internet unbemerkt abzufragen.⁵⁸

Diese Möglichkeiten können natürlich auch von Privatleuten oder Unternehmen ausgenutzt werden. Um dem vorzubeugen, sind in einigen Unternehmen Besprechungszimmer nicht mit Telefonanschlüssen und Netzwerkanschlüssen ausgestattet und Mobiltelefone müssen dort abgeschaltet werden.

3.2. Spione in der Geldbörse

Viele Spuren unseres Täglichen Lebens legen wir selbst und tragen zur Aufzeichnung derselben, zum Teil freiwillig, fleißig bei.

Um den Gebrauch der Krankenversichertenkarte kommt man, will oder muß man ärztliche Hilfe in Anspruch nehmen, nicht herum.⁵⁹ Unsere Volksvertretung hat dies so beschlossen. Beim Arzt anhand der

⁵⁵ Als Kommunikationselektroniker Fachrichtung Telekommunikationstechnik kenne ich Beispiele zur Fernwartung kleiner und großer Telekommunikationsanlagen aus der Praxis.

⁵⁶ Es gibt Systemtelefone, deren Funktion weitgehend von der Anlage bestimmt wird.

⁵⁷ Beim Bildtelefon T-View 100 der Deutschen Telekom läßt sich sogar die Kamera nahezu unbemerkt aktivieren - lediglich wenn man das Display und den Status der Leuchtdioden genau beobachtet, nimmt man dies wahr. Allerdings muß diese Funktion zuvor grundsätzlich am Gerät eingerichtet werden.

⁵⁸ Natürlich können dann auch sonstige auf diesem PC gespeicherte oder von diesem aus abfragbare Daten ausgespäht oder manipuliert werden.

⁵⁹ Dies gilt zumindest für Mitglieder der Gesetzlichen Krankenkassen.

Versichertennummer gespeicherte Daten werden jedoch nicht wirklich umfassend zentral verarbeitet.

Zur Abrechnung ärztlicher Leistungen werden durch die Kassenärztlichen Vereinigungen die Abrechnungsrelevanten Daten, die auch die den Fallpauschalen zugrundeliegenden maschinenlesbar codierten Diagnosen enthalten, von den eindeutigen Identifikatoren der Personenbezogenen Daten, wie Versicherungsnummer getrennt an die Kassen übermittelt. Die Reihenfolge wird hierbei geändert und ein Zusammenführen der Daten ist nicht erlaubt.⁶⁰ Die Verwendung derart erhobener Daten ist jedoch prinzipiell möglich und könnte Gegenstand künftiger Gesetze, zum Beispiel zur Kostenreduzierung im Gesundheitswesen werden.

Konto- oder Kreditkarten verwenden wir freiwillig, um bequem einkaufen zu können. Bei genauer Betrachtung fällt jedoch auf, daß in vielen Fällen, wie beim Versandhandel oder bei Mobilfunkverträgen oft keine Barzahlung akzeptiert wird. Auch Lohnzahlungen werden selten bar vorgenommen – anderes Vorgehen erweckt sofort den Verdacht von Schwarzarbeit. Da Kontoverbindungen eindeutige Identifikatoren darstellen, können Kartenzahlungen und Lastschriften bei Bedarf leicht zugeordnet werden. In erster Linie könnte man befürchten, daß Unternehmen Kundenprofile erstellen. Auf den Zweiten Blick könnte aber auch ein staatlicher Zugriff auf Kontoauszüge die Erstellung von Bewegungsprofilen oder anderen Verhaltensprofilen ermöglichen. Wer sich nach dem Attentat auf das World Trade Center politisch korrekt verhält, kauft natürlich nicht bei arabischen Onlinehändlern, sondern ißt aus reiner Solidarität in US-amerikanischen Schnellrestaurants.⁶¹

3.3. Videoüberwachung

Kameras im öffentlichen Bereich werden weitgehend akzeptiert und scheinen ein Stück weit ein Gefühl von Sicherheit zu vermitteln.

In London findet, so scheint es, eine flächendeckende Überwachung des öffentlichen Bereichs, zumindest an Brennpunkten, statt.⁶²

Betrachtet man die Situation in Frankfurt am Main, stellt man fest, daß es vielleicht keine flächendeckende Kameraüberwachung gibt, aber anscheinend

⁶⁰ Vertrag über den Datenaustausch auf Datenträgern (Anlage 6 BMV-Ä und EKV), http://www.kvhessen.de/documents_getdoc.cfm?pdfdoc=Anlage6Datenaustausc.pdf, 14.07.2003 / 14:43

⁶¹ Solcherlei Äußerungen gehören vielleicht nicht in eine Wissenschaftliche Arbeit, können aber Verwendungsmöglichkeiten solcher Daten aufzeigen.

⁶² Wer sich nun genau im Blickfeld der Kamera befindet und ob der Polizist am Monitor gerade blinzelt oder die Situation anders einschätzt, als sie ist, bleibt dem Publikum verborgen. Was außerhalb des Erfassungsbereiches der Kamera geschieht, zeichnet diese natürlich nicht auf...

wenigstens Bahnsteige der U- und S-Bahnstationen, einige öffentliche Plätze (z.B. Konstabler Wache), Parkhäuser und sämtliche Geldautomaten und Kassenräume von Banken und Sparkassen sowie viele Firmengelände überwacht werden. Diese vielen Kameras vermitteln wohl den Eindruck einer gewissen Überwachung öffentlichen Raumes, in Wirklichkeit dienen sie jedoch meistens keiner kontinuierlichen Überwachung oder unterstehen nicht unmittelbar staatlichem Zugriff.

Kameras im Bereich von Bahnsteigen sind fest auf die Bahnsteigkante ausgerichtet und dienen den Fahrern, teilweise auch anderem Bahnpersonal, z.B. in der Leitstelle, dazu, sicherzustellen, daß die Türen frei sind und beim Ausfahren niemand vom Zug mitgeschleift wird. Da so vor Allem Zugbegleiter eingespart werden, rechne ich nicht damit, daß diese Bilder aufgezeichnet werden und dann Datenschutzbeauftragte der Bahn über die weitere Verwendung und fristgerechte Löschung der Bänder wachen, wodurch wieder Personalkosten entstünden.

Kameras in Banken und Sparkassen zur Überwachung von Kassen- und Schalterräumen werden in der Regel nur auf Knopfdruck manuell ausgelöst, um einzelne oder eine Serie von Bildern aufzuzeichnen, oder im Falle eines Alarms automatisch aktiviert.⁶³ Diese Aufzeichnungen werden, ebenso wie die Aufzeichnungen von Kameras zur Überwachung von Geldautomaten, erst dann an staatliche Stellen übergeben, wenn anzunehmen ist, daß darauf eine Straftat zu beobachten ist.

In Unternehmen anfallende Aufzeichnungen werden, sofern sie ohne entsprechende Vorfälle überhaupt aufbewahrt und nicht automatisch überschrieben werden, in den Archiven verstauben, bis sie nach Ablauf interner Aufbewahrungsfristen, angelehnt an Datenschutzrichtlinien vernichtet werden – verantwortungsvollen Umgang mit datenschutzrechtlich relevantem Material vorausgesetzt...⁶⁴

Die Wirksamkeit der Kameraüberwachung zur Aufklärung von Straftaten oder zur Abschreckung stelle ich nicht in Frage, ebensowenig die Möglichkeit, daß vielleicht Straftaten an andere, nicht überwachte Orte verlagert werden.

So könnte man beispielsweise die Busse der Stadtverkehr Maintal GmbH betrachten, deren Inneneinrichtung, vor Allem im hinteren Bereich grundsätzlich bemalt, beschrieben und anderweitig beschädigt wurde. Als neue Busse ebenfalls erste Beschädigungen aufwiesen, wurden gut sichtbar Kameras, vielleicht aber auch nur Kameraattrappen an der Decke installiert, Hinweise in

⁶³ Viele Kassen und Schalter werden durch Kameras überwacht, die einen chemischen Film belichten, deshalb ist in diesen Fällen eine Dauerüberwachung gar nicht realisierbar.

⁶⁴ Wer überwacht, daß man dort nicht allzu sorglos Videobänder beim „Ausmisten“, beim Umzug oder Geschäftsauflösung einfach in den Müll schmeißt...?

der Nähe des Einstieges angebracht und die Busse in Stand gesetzt. Seitdem treten anscheinend keine Beschädigungen mehr auf.⁶⁵

Aus dieser Erfahrung heraus könnte man natürlich ganze Städte mit Kameras übersäen. Billige schwarzweiß - Kameramodule konnte ich bereits für 10 Euro erwerben.⁶⁶ Bei diesem Preis könnte es sich lohnen, jeden von Vandalismus betroffenen Bereich zu überwachen und auf Video aufzuzeichnen, geeignete Langzeit-Videorecorder gibt es auch schon für weniger, als 2000 Euro...

Ob dies gewünscht ist, scheint aber nicht nur von Wirksamkeit und Wirtschaftlichkeit abzuhängen.

3.4. Satellitengestützte Überwachung

Die Leistungsfähigkeit moderner Objektive und Kameras sowie anderer bildgebender Verfahren gibt Anlaß zu der Annahme, es sei leicht, von einem Satelliten aus sogar die Zeitung eines Passanten zu lesen. Wolken und Atmosphäre beeinträchtigen jedoch die Bildqualität durch Dämpfung und Brechung des Lichtes, aber auch anderer elektromagnetischer Wellen, wie Radarstrahlen.

Trotz Allem gibt es sogar kommerzielle Satelliten, wie IKONOS⁶⁷, dessen Bilder eine Auflösung von einem Meter aufweisen. Betrachtet man beispielsweise ein Bild des Flughafens Frankfurt⁶⁸, so kann man hierauf sogar einzelne PKW erahnen. Dies genügt noch lange nicht, um einzelne Personen zu erkennen, aber militärische Satelliten dürften aufgrund Jahrzehntelanger Entwicklungszeiten und Erfahrungen vielleicht sogar bessere Auflösungen aufweisen. Ich hörte und las, ohne die Quellen überprüfen zu können, von Auflösungen von 10 Zentimetern und weniger.

Texte zu lesen dürfte jedoch aufgrund Atmosphärischer Störungen derzeit vom Satelliten aus unmöglich sein. Allein Schwankungen in der atmosphärischen Dichte verschlechtern das Bild derart, daß verschiedene bildgebende Verfahren, zum Beispiel optische Bilder verschiedener Wellenlänge, kombiniert werden müssen, um die erstaunlich guten Fotos von IKONOS zu erhalten.

Ob vor einem Gebäude ein PKW steht und ob sein Motor Wärme abstrahlt, also kürzlich lief oder noch läuft, kann man aufgrund solcher Daten sicher ermitteln. Wenn der vermutete Technologievorsprung militärischer Systeme zutrifft, ist

⁶⁵ Da ich in Maintal wohne und diese Bussen fast täglich nutze, konnte ich dies selbst beobachten.

⁶⁶ Kameramodul ohne Gehäuse und Stromversorgung für 9,99 € bei Conrad Electronic.

⁶⁷ siehe <http://www.spaceimaging.com>

⁶⁸ kostenlos abrufbares Beispiel:

http://www.spaceimaging.com/graphics/products/ikonos_examples/frankfurt.htm, 17.07.2003 / 12:36

sogar der Fahrzeugtyp feststellbar. Über zusätzliche Informationen, wie die Funkzelle eines aktiven Mobiltelefons, läßt sich diese Information weiter präzisieren.

3.5. Großer Lauschangriff

Eigentlich nicht Thema meiner Arbeit führe ich diese Problematik kurz an, da sie dennoch eng damit verwoben ist.

Analog zum Brief-, Post- und Fernmeldegeheimnis ist auch die Wohnung geschützt, so bestimmt Artikel 13 des Grundgesetzes:

„(1) Die Wohnung ist unverletzlich.“⁶⁹

Neben der TKÜV werden ganz besonders die 1998 in Artikel 13 eingefügten Absätze 3-6 unter dem Thema „Großer Lauschangriff“ diskutiert. Absatz 3 führe ich hier auszugsweise an:

„Begründen bestimmte Tatsachen den Verdacht, daß jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat, so dürfen zur Verfolgung der Tat auf Grund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden, wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. [...]“⁷⁰

Zwar sind auch hier richterliche Hürden vorgesehen, aber der Umstand, daß der begründete Verdacht genügt, ein die Erfordernisse dieses Gesetzes erfüllender Straftäter halte sich in einer Wohnung auf, um eine Wohnung mit „Wanzen“ zu bestücken, läßt etliche Menschen hier den Beginn eines Überwachungsstaates nach Orwells „Big Brother“ vermuten.

4. Kein Grund zu Paranoia

Telefonate und andere übermittelte Nachrichten abzuhören und aufzuzeichnen ist aus technischer Sicht einfach. Die technischen Möglichkeiten George Orwells 1984 sind längst überholt.

Heute kann man davon ausgehen, daß von der Beantragung über die Einrichtung bis zur Auswertung von Überwachungsmaßnahmen ein gewisser finanzieller und, vor Allem bei der Auswertung, personeller Aufwand notwendig ist. Künftige Entwicklungen, wie der Quantencomputer, falls es ihn geben wird, könnten dies vielleicht ändern.

⁶⁹ Art 13 Grundgesetz, Stand 15.10.2002, Absatz 1

⁷⁰ Art 13 Grundgesetz, Stand 15.10.2002, Absatz 3

Die Wirksamkeit der Methoden zur Überwachung und zur Auswertung gesammelter Daten wird sich, einen kontinuierlichen Fortschritt vorausgesetzt, von selbst verbessern. Die technischen Hürden werden also weiter schwinden.

In welchem Grad der Überwachungsstaat sich verwirklicht, hängt jedoch maßgeblich davon ab, welche Meinung sich die Öffentlichkeit bildet und wie streng sie auf die Umsetzung in der Gesetzgebung und die Anwendung dieser Gesetze achtet.

Nicht alles, was möglich ist, wird auch flächendeckend eingesetzt. Aber Aufmerksamkeit ist angebracht. Die Gefahren liegen nicht in der Technik selbst, sondern in unserem Umgang mit ihr.

„Ich habe nichts zu verbergen!“ könnte sorgloser Ausdruck der Ansicht eines unbescholtenen, aufrichtigen Bürgers sein oder die verinnerlichte Forderung eines allgegenwärtigen Großen Bruders.

Egal ob es sich um Spuren im Staub oder elektronische Fährten handelt, wir hinterlassen Hinweise auf unser Handeln – inwieweit wir anderen erlauben, diese Hinweise zu verwerten, ist eine soziale Frage, die weder von einem technischen Standpunkt aus noch stellvertretend beantwortet werden kann, sondern von der Gesellschaft aufgegriffen und diskutiert werden muß.

Danksagung

Mein Dank gilt

- meinen Eltern für die finanzielle Unterstützung und den Transport der Materialien für den Schauversuch vom 13.05.2003,
- Herrn Rohner, der mir seine alte Telefonanlage schenkte,
- Thorsten König für die Hilfe beim Aufbau und die Bewachung meiner Geräte,
- Herrn Simon, der mir Diaprojektor, Videokamera und Stativ unbürokratisch zur Verfügung stellte und mich kurz in die Bedienung der audiovisuellen Anlage einwies,
- Herrn Mans, der mir auf meinen Wunsch diesen frühen Termin für meinen Schauversuch außerplanmäßig überließ und die Veranstaltung wohlwollend begleitete
- und den bis zuletzt aufmerksamen Seminarteilnehmern.

Urheberrechtlicher Hinweis

(c) 2003 Murad Khasawneh,

Jede Nutzung über die vom Urheberrechtsgesetz eingeräumten Rechte hinaus bedarf der ausdrücklichen Zustimmung des Urhebers.⁷¹

Letzte Aktualisierung: 18.07.2003, 09:57 Uhr

Achtung: Die ausnahmslose Ausfertigung dieser Arbeit in deutscher Sprache ist Teil eines Konzeptes, das die Verbreitung der Dokumente regulieren und auf den deutschsprachigen Raum begrenzen soll. Dies bezeichne ich ausdrücklich als Kopierschutz. Jede Übersetzung ohne meine Einwilligung werde ich als Verstoß gegen geltendes Urheberrecht, das ausdrücklich das Recht zur Regulierung der Verbreitung eines Werkes durch den Urheber vorsieht.

⁷¹ Bei Fragen zum Gesetzestext wenden Sie sich bitte an den Rechtsberater Ihrer Wahl oder den Gesetzgeber. Darüber hinausgehende Nutzungsrechte erteilt der Urheber im Einzelfall schriftlich.